IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 09/288,462
Filing Date ..... April 8, 1999
Inventor.....Richard Harrington, et al.
Group Art Unit 2132
Examiner .....Lanier, Benjamin
Attorney's Docket No. MS1-827US
Confirmation No. 7531
Title: Encrypted Software Installer

APPEAL BRIEF

To: Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

From: Allan Sponseller (Tel. 509-324-9256x215; Fax 509-323-8979)
Customer No. 22801

Pursuant to 37 C.F.R. §41.37, Applicant hereby submits an appeal brief for application 09/288,462, filed April 8, 1999, within the requisite time from the date of filing the Notice of Appeal. Accordingly, Applicant appeals to the Board of Patent Appeals and Interferences seeking review of the Examiner's rejections.

(1) Real Party in Interest

The real party in interest is Microsoft Corporation, the assignee of all right, title and interest in and to the subject invention.

(2) Related Appeals and Interferences

Appellant is not aware of any other appeals, interferences, or judicial proceedings which will directly affect, be directly affected by, or otherwise have a bearing on the Board's decision to this pending appeal.

(3) Status of Claims

Claims 1-8 stand rejected and are pending in this Application. Claims 1-8 are appealed. Some of claims 1-8 were previously amended. Claims 9-36 were previously canceled. Claims 1-8 are set forth in the Appendix of Appealed Claims on page 19.

(4) Status of Amendments

A Final Office Action was issued on July 1, 2005.

A Response to the Final Office Action was filed December 1, 2005. Claims 1 and 8 were amended as part of this Response.

An Advisory Action was issued on December 20, 2005, indicating that the request for reconsideration had been considered but did not place the application in condition for allowance. The Advisory Action further indicated that for purposes of appeal, the proposed amendment(s) in the Response to the Final Office Action will be entered.

Appellant filed a Notice of Appeal on January 3, 2006 in response to the Advisory Action and the Final Office Action.

(5) Summary of Claimed Subject Matter

A concise explanation of each of the independent claims is included in this Summary section, including specific reference characters. These specific reference characters are examples of particular elements of the drawings for certain embodiments of the claimed invention, and the claims are not limited to solely the elements corresponding to these reference characters.

With respect to independent claim 1, as discussed for example at page 11, line 3 through page 17, line 9, an installation module (202) comprises an encrypted software module (225), a decryption key (304), and an executive (215). The encrypted software module (225) is a first version of the software module. The decryption key (304) is to decrypt the encrypted software module (225), and the decryption key (225) is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm. The executive (215) uses the decryption key (304) to decrypt the encrypted software module (225) when at least one of a set of trigger files is stored on a computing system (20) and also installs the first version of the software module on the computing system (20) when at least one of the set of trigger files is stored on the computing system (20). Each of the trigger files indicates authorization to install the encrypted software module (225), and the first version of the software module uses greater than a threshold strength encryption. A second version of the software module is installed if at least one of the set of trigger files is not stored on

the computing system (20), and the second version of the software module uses a strength encryption that is not greater than the threshold strength encryption.

With respect to independent claim 2, as discussed for example at page 11, line 3 through page 17, line 9, an installation module (202) comprises an encrypted software module (225), a key (304), an executive (215), and a database (220). The database (220) identifies trigger files. The key (304) is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm. The executive (215) decrypts and installs the encrypted software module (225) with the key (304) when at least one of a set of trigger files is stored on a computing system (20). The encrypted software module (225) uses greater than a threshold strength encryption, and a different version of the software module is installed when at least one of the set of trigger files is not stored on the computing system (20). This different version of the software module uses a strength encryption that is not greater than the threshold strength encryption.

(6) Grounds of Rejection to be Reviewed on Appeal

Claims 1-3 and 8 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,530,752 to Rubin in view of U.S. Patent No. 6,075,862 to Yoshida et al. and further in view of U.S. Patent No. 6,473,860 to Chan.

Claims 4 and 6 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,530,752 to Rubin in view of U.S. Patent No.

6,075,862 to Yoshida et al. and further in view of U.S. Patent No. 6,473,860 to Chan and further in view of U.S. Patent No. 6,058,478 to Davis.

Claim 7 stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,530,752 to Rubin in view of U.S. Patent No. 6,075,862 to Yoshida et al. and further in view of U.S. Patent No. 6,473,860 to Chan and further in view of U.S. Patent No. 6,058,478 to Davis and further in view of U.S. Patent No. 5,825,890 to Elgamal et al.

Claim 5 stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,530,752 to Rubin in view of U.S. Patent No. 6,075,862 to Yoshida et al. and further in view of U.S. Patent No. 6,473,860 to Chan and further in view of U.S. Patent No. 5,199,073 to Scott.

(7) Argument

A. Rejection under 35 U.S.C. §103(a) over U.S. Patent No. 5,530,752 to Rubin in view of U.S. Patent No. 6,075,862 to Yoshida et al. and further in view of U.S. Patent No. 6,473,860 to Chan.

Claims 1-3 and 8 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,530,752 to Rubin (hereinafter "Rubin") in view of U.S. Patent No. 6,075,862 to Yoshida et al. (hereinafter "Yoshida") and further in view of U.S. Patent No. 6,473,860 to Chan (hereinafter "Chan").

1. Claims 1 and 8

With respect to claim 1, claim 1 recites:

An installation module comprising:

an encrypted software module that is a first version of the software module;

a decryption key to decrypt the encrypted software module, wherein the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm; and

an executive for using the decryption key to decrypt the encrypted software module when at least one of a set of trigger files is stored on a computing system and to install the first version of the software module on the computing system when at least one of the set of trigger files is stored on the computing system, wherein each of the trigger files indicates authorization to install the encrypted software module, and wherein the first version of the software module uses greater than a threshold strength encryption;

wherein a second version of the software module is installed if at least one of the set of trigger files is not stored on the computing system, and wherein the second version of the software module uses a strength encryption that is not greater than the threshold strength encryption.

In the Response to the Final Office Action, claim 1 was amended to incorporate the elements of its dependent claim 35. In the July 1, 2005 Final Office Action, claim 35 was rejected under 35 U.S.C. §103(a) as being unpatentable over Rubin in view of Yoshida and further in view of Chan and U.S. Patent No. 6,058,478 to Davis (hereinafter "Davis") and further in view of U.S. Patent No. 6,192,474 to Patel (hereinafter "Patel '474").

In the July 1, 2005 Final Office Action at p. 8 and the December 20, 2005 Advisory Action at p. 2, Patel '474 at col. 2, lines 37-59 is cited as disclosing using a hash of authentication information as an encryption key. The cited portion of Patel '474 discusses calculating a value ($g^{R_M R_N}$ mod p) as part of a Diffie-Hellman Encrypted Key Exchange and using a hash thereof as a session key (see, col. 2, lines 56-69). However, in the July 1, 2005 Office Action at pp. 4-5, the decryption key 305 of Rubin is relied on as disclosing the decryption key of

claim 1 while the version number from the Executable Object Code System Program of Rubin is relied on as disclosing the at least one of a set of trigger files of claim 1 (see, July 1, 2005 Office Action at pp. 4-5). Thus, in order to satisfy the language of claim 1, there would need to be some disclosure or suggestion to encrypt the decryption key 305 of Rubin as a function of a cryptographic hash value produced by hashing the version number of Rubin. Applicant respectfully submits that the mere discussion of using a hash of a value calculated as part of a Diffie-Hellman Encrypted Key Exchange as a session key in Patel '474 does not provide any disclosure or suggestion of hashing the version number of Rubin, much less of using the resulting hash value to encrypt a decryption key. There is no discussion or mention in Rubin or Patel '474 to use a value derived from a trigger file to encrypt a decryption key, much less of the decryption key being encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm. Without any such discussion or mention, Applicant respectfully submits that Rubin and Patel '474 cannot disclose or suggest a decryption key to decrypt the encrypted software module, wherein the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm as recited in claim 1.

Furthermore, in the July 1, 2005 Final Office Action at p. 3 and the December 20, 2005 Advisory Action at p. 2, it was asserted that it would have been obvious to one of ordinary skill in the art at the time the invention was made to use a hash value as an encryption key in Davis in order to add security prior to establishing the key as taught in Patel (Col. 3, lines 36-38). However, there still is no assertion that a hash value is produced by hashing a corresponding trigger file

as recited in claim 1. As the version number from the Executable Object Code System Program of Rubin is relied on as disclosing the at least one of a set of trigger files of claim 1, Applicant respectfully submits that in order to disclose the elements of claim 1 there must be some disclosure or suggestion that a decryption key is encrypted as a function of a cryptographic hash value produced by hashing a version number with a hash algorithm. As there is no discussion or mention of hashing the version number of Rubin or of why one would want to hash the version number of Rubin, much less of using the hashed version number or of why one would want to use the hashed version number for encrypting the decryption key, Applicant respectfully submits that Rubin in view of Patel '474 cannot disclose or suggest wherein a decryption key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm as recited in claim 1.

Yoshida, Chan, and Davis are not cited as curing, and do not cure, these deficiencies of Rubin in view of Patel '474.

In addition, in the July 1, 2005 Final Office Action at p. 3 and the December 20, 2005 Advisory Action at p. 2, it was asserted that it would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the decryption key in the protected software system of Rubin in order to authenticate the sender of the information as taught in Davis (Col. 3, lines 60-64). As discussed above, however, in order to disclose the elements of claim 1 there must be some disclosure or suggestion that the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a version number with a hash algorithm. Applicant respectfully submits that a hash of a version number

does not authenticate any sender of information, and thus that there is no suggestion that the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a version number with a hash algorithm in the cited references. Accordingly, for at least these reasons, Applicant respectfully submits that the cited references do not disclose or suggest a decryption key to decrypt the encrypted software module, wherein the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm as recited in claim 1.

In the December 20, 2005 Advisory Action, it was indicated that the request for reconsideration had been considered but did not place the application in condition for allowance because:

> In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Applicant's arguments attack each reference individually and fail to take into account the combined teachings of the references.

Appellant respectfully submits that the combination of Rubin, Yoshida, Chan, Davis, and Patel '474 has been addressed above. Appellant is not attacking references individually. Appellant is relying on the rejections made in the July 1, 2005 Final Office Action and the assertions made in the July 1, 2005 Final Office Action as to where the elements of claim 1 are allegedly taught in Rubin, Yoshida, Chan, Davis, and Patel '474. As discussed above, all the elements of claim 1 are not taught or suggested by the combination of Rubin, Yoshida, Chan, Davis, and Patel '474.

Accordingly, for at least these reasons, Applicant respectfully submits that claim 1 is allowable over Rubin in view of Yoshida and further in view of Chan and further in view of Davis and further in view of Patel '474.

With respect to claim 8, given that claim 8 depends from claim 1, Applicant respectfully submits that claim 8 is allowable over Rubin in view of Yoshida and further in view of Chan and further in view of Davis and further in view of Patel '474 for at least the reasons discussed above with respect to claim 1.

2. Claims 2 and 3

With respect to claim 2, claim 2 recites:

> An installation module comprising:
> an encrypted software module;
> a key, wherein the key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm;
> an executive for decrypting and installing the encrypted software module with the key when at least one of a set of trigger files is stored on a computing system, wherein the encrypted software module uses greater than a threshold strength encryption, wherein a different version of the software module is installed when at least one of the set of trigger files is not stored on the computing system, and wherein the different version of the software module uses a strength encryption that is not greater than the threshold strength encryption; and
> a database for identifying the trigger files.

In the Response to the Final Office Action, claim 2 was amended to incorporate the elements of its dependent claim 36. In the July 1, 2005 Final Office Action, claim 36 was rejected under 35 U.S.C. §103(a) as being unpatentable over Rubin in view of Yoshida and further in view of Chan and U.S. Patent No. 6,058,478 to

Davis (hereinafter "Davis") and further in view of U.S. Patent No. 6,192,474 to Patel (hereinafter "Patel '474").

In the July 1, 2005 Final Office Action at p. 8 and the December 20, 2005 Advisory Action at p. 2, Patel '474 at col. 2, lines 37-59 is cited as disclosing using a hash of authentication information as an encryption key. The cited portion of Patel '474 discusses calculating a value ($g^{R_M R_N}$ mod p) as part of a Diffie-Hellman Encrypted Key Exchange and using a hash thereof as a session key (see, col. 2, lines 56-69). However, in the July 1, 2005 Office Action at pp. 4-5, the decryption key 305 of Rubin is relied on as disclosing the key of claim 2 while the version number from the Executable Object Code System Program of Rubin is relied on as disclosing the at least one of a set of trigger files of claim 2 (see, July 1, 2005 Office Action at pp. 4-5). Thus, in order to satisfy the language of claim 2, there would need to be some disclosure or suggestion to encrypt the decryption key 305 of Rubin as a function of a cryptographic hash value produced by hashing the version number of Rubin. Applicant respectfully submits that the mere discussion of using a hash of a value calculated as part of a Diffie-Hellman Encrypted Key Exchange as a session key in Patel '474 does not provide any disclosure or suggestion of hashing the version number of Rubin, much less of using the resulting hash value to encrypt a key. There is no discussion or mention in Rubin or Patel '474 to use a value derived from a trigger file to encrypt a key, much less of the key being encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm. Without any such discussion or mention, Applicant respectfully submits that Rubin and Patel '474 cannot disclose or suggest a key, wherein the key is encrypted as a

function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm as recited in claim 2.

Furthermore, in the July 1, 2005 Final Office Action at p. 3 and the December 20, 2005 Advisory Action at p. 2, it was asserted that it would have been obvious to one of ordinary skill in the art at the time the invention was made to use a hash value as an encryption key in Davis in order to add security prior to establishing the key as taught in Patel (Col. 3, lines 36-38). However, there still is no assertion that a hash value is produced by hashing a corresponding trigger file as recited in claim 2. As the version number from the Executable Object Code System Program of Rubin is relied on as disclosing the at least one of a set of trigger files of claim 2, Applicant respectfully submits that in order to disclose the elements of claim 2 there must be some disclosure or suggestion that the key is encrypted as a function of a cryptographic hash value produced by hashing a version number with a hash algorithm. As there is no discussion or mention of hashing the version number of Rubin or of why one would want to hash the version number of Rubin, much less of using the hashed version number or of why one would want to use the hashed version number for encrypting the decryption key, Applicant respectfully submits that Rubin in view of Patel '474 cannot disclose or suggest wherein a key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm as recited in claim 2.

Yoshida, Chan, and Davis are not cited as curing, and do not cure, these deficiencies of Rubin in view of Patel '474.

In addition, in the July 1, 2005 Final Office Action at p. 3 and the December 20, 2005 Advisory Action at p. 2, it was asserted that it would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the decryption key in the protected software system of Rubin in order to authenticate the sender of the information as taught in Davis (Col. 3, lines 60-64). As discussed above, however, in order to disclose the elements of claim 2 there must be some disclosure or suggestion that the key is encrypted as a function of a cryptographic hash value produced by hashing a version number with a hash algorithm. Applicant respectfully submits that a hash of a version number does not authenticate any sender of information, and thus that there is no suggestion that the key is encrypted as a function of a cryptographic hash value produced by hashing a version number with a hash algorithm in the cited references. Accordingly, for at least these reasons, Applicant respectfully submits that the cited references do not disclose or suggest a key, wherein the key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm as recited in claim 2.

In the December 20, 2005 Advisory Action, it was indicated that the request for reconsideration had been considered but did not place the application in condition for allowance because:

> In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Applicant's arguments attack each reference individually and fail to take into account the combined teachings of the references.

Appellant respectfully submits that the combination of Rubin, Yoshida, Chan, Davis, and Patel '474 has been addressed above. Appellant is not attacking references individually. Appellant is relying on the rejections made in the July 1, 2005 Final Office Action and the assertions made in the July 1, 2005 Final Office Action as to where the elements of claim 2 are allegedly taught in Rubin, Yoshida, Chan, Davis, and Patel '474. As discussed above, all the elements of claim 1 are not taught or suggested by the combination of Rubin, Yoshida, Chan, Davis, and Patel '474.

Accordingly, for at least these reasons, Applicant respectfully submits that claim 2 is allowable over Rubin in view of Yoshida and further in view of Chan and further in view of Davis and further in view of Patel '474.

With respect to claim 3, given that claim 3 depends from claim 2, Applicant respectfully submits that claim 3 is allowable over Rubin in view of Yoshida and further in view of Chan and further in view of Davis and further in view of Patel '474 for at least the reasons discussed above with respect to claim 2.

B. Rejection under 35 U.S.C. §103(a) over U.S. Patent No. 5,530,752 to Rubin in view of U.S. Patent No. 6,075,862 to Yoshida et al. and further in view of U.S. Patent No. 6,473,860 to Chan and further in view of U.S. Patent No. 6,058,478 to Davis.

Claims 4 and 6 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,530,752 to Rubin (hereinafter "Rubin") in view of U.S. Patent No. 6,075,862 to Yoshida et al. (hereinafter "Yoshida") and

further in view of U.S. Patent No. 6,473,860 to Chan (hereinafter "Chan") and further in view of U.S. Patent No. 6,058,478 to Davis (hereinafter "Davis").

1. Claims 4 and 6

Claims 4 and 6 depend from independent claims 2 and 1, respectively. Applicant respectfully submits that claims 4 and 6 are allowable over Rubin in view of Yoshida and further in view of Chan and further in view of Davis for at least the reasons discussed above with respect to claims 2 and 1, respectively.

C. Rejection under 35 U.S.C. §103(a) over U.S. Patent No. 5,530,752 to Rubin in view of U.S. Patent No. 6,075,862 to Yoshida et al. and further in view of U.S. Patent No. 6,473,860 to Chan and further in view of U.S. Patent No. 6,058,478 to Davis and further in view of U.S. Patent No. 5,825,890 to Elgamal et al.

Claim 7 stands rejected under 35 U.S.C. §103(a) as being unpatentable over R U.S. Patent No. 5,530,752 to Rubin (hereinafter "Rubin") in view of U.S. Patent No. 6,075,862 to Yoshida et al. (hereinafter "Yoshida") and further in view of U.S. Patent No. 6,473,860 to Chan (hereinafter "Chan") and further in view of U.S. Patent No. 6,058,478 to Davis (hereinafter "Davis") and further in view of U.S. Patent No. 5,825,890 to Elgamal et al. (hereinafter "Elgamal").

1. Claim 7

Claim 7 depends from claim 6. Applicant respectfully submits that claim 7 is allowable over Rubin in view of Yoshida and further in view of Chan and

further in view of Davis at least because of its dependency on claim 6. Elgamal is not cited as curing, and does not cure, the deficiencies of Rubin in view of Yoshida and further in view of Chan and further in view of Davis discussed above with respect to claim 6. For at least these reasons, Applicant respectfully submits that claim 7 is allowable over Rubin in view of Yoshida and further in view of Chan and further in view of Davis and further in view of Elgamal.

D. Rejection under 35 U.S.C. §103(a) over U.S. Patent No. 5,530,752 to Rubin in view of U.S. Patent No. 6,075,862 to Yoshida et al. and further in view of U.S. Patent No. 6,473,860 to Chan and further in view of U.S. Patent No. 5,199,073 to Scott.

Claim 5 stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,530,752 to Rubin (hereinafter "Rubin") in view of U.S. Patent No. 6,075,862 to Yoshida et al. (hereinafter "Yoshida") and further in view of U.S. Patent No. 6,473,860 to Chan (hereinafter "Chan") and further in view of U.S. Patent No. 5,199,073 to Scott (hereinafter "Scott").

1. Claim 5

Claim 5 depends from independent claim 2. Applicant respectfully submits that claim 5 is allowable over Rubin in view of Yoshida and further in view of Chan at least because of its dependency on claim 2. Scott is not cited as curing, and does not cure, the deficiencies of Rubin in view of Yoshida and further in view of Chan discussed above with respect to claim 2. For at least these reasons,

Applicant respectfully submits that claim 5 is allowable over Rubin in view of Yoshida and further in view of Chan and further in view of Scott.

Conclusion

The Office's basis and supporting rationale for the § 103(a) rejections is not supported by the teaching of the cited references. Applicant respectfully requests that the rejections be overturned and that pending claims 1-8 be allowed to issue.

Respectfully Submitted,

Dated: 6/5/06

By: _____

Allan T. Sponseller
Lee & Hayes, PLLC
Reg. No. 38,318
(509) 324-9256 ext. 215

(8) Appendix of Appealed Claims

1. An installation module comprising:

an encrypted software module that is a first version of the software module;

a decryption key to decrypt the encrypted software module, wherein the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm; and

an executive for using the decryption key to decrypt the encrypted software module when at least one of a set of trigger files is stored on a computing system and to install the first version of the software module on the computing system when at least one of the set of trigger files is stored on the computing system, wherein each of the trigger files indicates authorization to install the encrypted software module, and wherein the first version of the software module uses greater than a threshold strength encryption;

wherein a second version of the software module is installed if at least one of the set of trigger files is not stored on the computing system, and wherein the second version of the software module uses a strength encryption that is not greater than the threshold strength encryption.

2. An installation module comprising:

an encrypted software module;

a key, wherein the key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm;

an executive for decrypting and installing the encrypted software module with the key when at least one of a set of trigger files is stored on a computing

system, wherein the encrypted software module uses greater than a threshold strength encryption, wherein a different version of the software module is installed when at least one of the set of trigger files is not stored on the computing system, and wherein the different version of the software module uses a strength encryption that is not greater than the threshold strength encryption; and

a database for identifying the trigger files.

3. The installation module of claim 2, wherein the database includes the key.

4. The installation module of claim 3, wherein the key is encrypted.

5. The installation module of claim 2, wherein the database includes a hash value for each of the trigger files.

6. The system of claim 1, wherein the encrypted software module is a cryptographic software module.

7. The system of claim 6, wherein the encrypted software module is a dynamic-link library (DLL) for providing a secure socket layer (SSL).

8. The system of claim 1, wherein the encrypted software module resides on a computer-readable medium.

(9) Appendix of Evidence Submitted

None.

(10) Appendix of Related Proceedings

None.